From: Bryan Mullins [b.mullins@ny.tr.mufg.jp]
Sent: Friday, December 29, 2006 1:40 PM
To: Taskforcecomments
Subject: Identity Theft

I applaud the committees efforts in pursuing a workable solution to a national crisis. Bravo.

Bryan Mullins
Vice-President
Risk Management and Analysis Group
Mitsubishi UFJ Trust and Banking Corporation
Direct: 212-891-8383

Recommendations for the Prevention of Identity Theft

1. **The use of authentication code on the back of an individual's credit card at retail establishments.** I have noticed recently that when a purchase is made at some retail establishments, the authentication codes located on the back of the credit card are typed into the register/computer system at checkout. Although this process is used when ordering items on the internet, typically the legitimate internet web-site payment systems are protected (such as using Verisign, PayPal, etc.) and the information is encoded before being processed. This is NOT true at the retail outlet level. This authentication code is written into the magnetic strip on the credit card and SHOULD NOT be re-input manually. This exposes each consumer to additional identity theft hazards from an unprotected internal computer system as well as prying eyes of a temporary retail clerk from having access to both the credit card number and the authentication code. The authentication code SHOULD NOT be a replacement to signatures and proper secondary identification.

2. **A mandatory requirement of credit card issuers to use an unusual activity program to identify possible fraud.** Some credit card issuers instituted a policy years ago of tracking the unusual activity of an individual's credit card account to identify possible fraudulent usage. However, that voluntary policy has either been abandoned or neglected recently. I know this from my own unusual activity. I used a credit card over the past two months that I have not used regularly for at least two years. The amount of purchases totaled more than $5,000. My credit card issuer DID NOT contact me or question the unusual activity. When I contacted them about my concern, they informed me that they usually do follow such unusual activity and apologized for their oversight. I was not convinced of their honest diligence. Since the introduction of the US Patriot Act and its inclusion of the Bank Secrecy Act, all financial institutions are REQUIRED to have in place a Customer Identification Policy that includes tracking unusual activity in corporate accounts. This policy should be expanded to include individual accounts, such as credit cards and bank accounts, with substantial penalties for those institutions that do not comply. One penalty might be the total replacement of all loses incurred by an individual, regardless if those losses are incurred at another institution, when the reason for those losses can be traced back to original non-compliance.

3. **The elimination of Social Security Numbers as a means of identification for non-financial transactions.** Too many non-financial institutions are utilizing and individual's SSN as their main identification for car insurance, health-care benefits and employee ID cards. This number is issued by the US Government to identify individuals for retirement benefits. However, the SSN has become the main tool of identification and has become incorporated into policy numbers and ID cards that have no reasonable reason to use the SSN. Many organizations have voluntary ceased using the SSN as their main identification, but voluntary policy changes are not always adhered to. A mandatory law must be instituted, again, including substantial penalties and liabilities for those organizations that do not comply.

4. **Enhanced identification systems, such as retina scanning and electronic fingerprint identification.** The newest technologies allow for retina scanning and fingerprint identification to be done quickly, efficiently and at reduced costs from even two or three years ago. Every US Citizen should be willing to submit to an identification method that can be stored in a secured database that can be accessed by authorized agencies and organizations. The identification process can be used at banks, airports, health-care facilities and federal, state and local government buildings. Of course some individuals might view this as an infringement on their first amendment rights, but it would solidify their position as a US citizen and add to the overall security of the country. Without actually mandating individuals submit to this type of identification, making it impossible to travel on a plane or enter a hospital without this type of identification method would dictate that everyone comply. And yet, they, as individuals, still have the right to refuse without penalty.